SIMULASI SERANGAN DOS

(hping3 & slowloris)

OLEH:

NAMA : ANDINI FEBRIANTI

KELAS : 5D

NIM : 105841113223

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

A. PENDAHULUAN UMUM

Ketersediaan layanan (availability) merupakan salah satu pilar utama dalam keamanan informasi, khususnya pada layanan berbasis web yang harus dapat diakses secara kontinu oleh pengguna. Salah satu ancaman serius terhadap aspek ini adalah serangan Denial of Service (DoS), yaitu serangan yang bertujuan membuat layanan tidak dapat digunakan dengan cara menghabiskan sumber daya sistem atau koneksi jaringan.

Pada praktikum ini dilakukan simulasi serangan DoS menggunakan dua pendekatan berbeda, yaitu SYN Flood pada *network layer* dan Slowloris pada *application layer*. Selain mengamati dampak serangan terhadap layanan web DVWA, praktikum ini juga menguji penerapan mitigasi firewall menggunakan IPTables untuk memulihkan layanan dan membedakan akses antara penyerang dan pengguna sah.

B. TUJUAN KEGIATAN

Tujuan dari praktikum ini adalah sebagai berikut:

1. Mensimulasikan serangan DoS jenis SYN Flood dan Slowloris pada layanan web.
2. Menganalisis dampak serangan terhadap ketersediaan layanan web DVWA.
3. Menguji efektivitas firewall IPTables dalam memitigasi serangan DoS.
4. Membandingkan kondisi akses layanan sebelum dan sesudah mitigasi diterapkan.

C. LINGKUNGAN DAN PERANGKAT YANG DIGUNAKAN

- Kali Linux (Rolling) – mesin attacker
- Ubuntu Server 20.04 / 22.04 – mesin target
- Apache2 – web server
- MariaDB – database DVWA
- PHP 7.x / 8.x – backend DVWA
- DVWA (Latest) – aplikasi target
- Hping3 – serangan SYN Flood
- Slowloris – serangan DoS layer aplikasi
- IPTables – firewall mitigasi
- VMware Workstation – virtualisasi lingkungan

- Mozilla Firefox – pengujian akses web

D. DESAIN SKENARIO PENGUJIAN

1. Topologi Jaringan

   Simulasi dilakukan menggunakan VMware Workstation dengan mode NAT, sehingga seluruh mesin berada pada satu segmen jaringan lokal yang terisolasi.

   Konfigurasi IP:

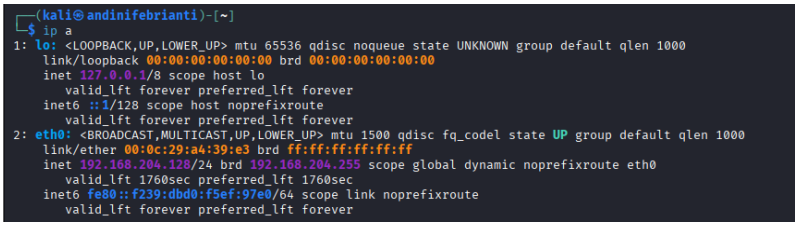
   - Attacker (Kali Linux) → 192.168.204.128
   - Target (Ubuntu Server) → 192.168.204.129

   Topologi ini memungkinkan serangan dilakukan secara langsung tanpa mekanisme routing tambahan.

E. VERIFIKASI KONFIGURASI JARINGAN

1. Mesin Attacker

   Hasil perintah ip a pada Kali Linux menunjukkan interface jaringan aktif dengan alamat IP 192.168.204.128/24. Hal ini memastikan attacker telah terhubung dengan benar ke jaringan simulasi.

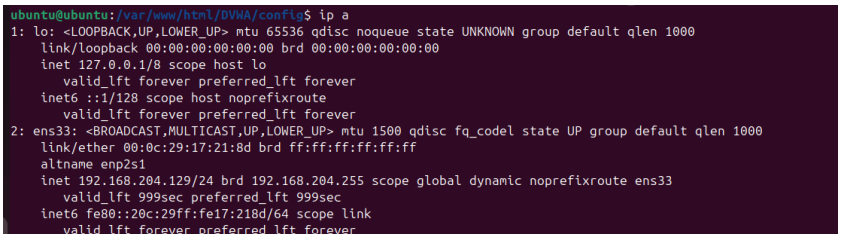


Gambar 1.1 Output Perintah ip a pada Mesin Attacker (Kali Linux)

Gambar 1.1 menampilkan hasil perintah ip a pada Kali Linux yang menunjukkan interface eth0 dalam keadaan UP dengan alamat IP 192.168.204.128/24 dan broadcast 192.168.204.255, menandakan mesin attacker telah terhubung ke jaringan NAT praktikum dan berada pada subnet yang sama dengan server target

2. Mesin Target

   Output ip a pada Ubuntu Server memperlihatkan interface ens33 dalam kondisi UP dengan alamat IP 192.168.204.129/24, menandakan target berada dalam satu subnet dengan attacker.

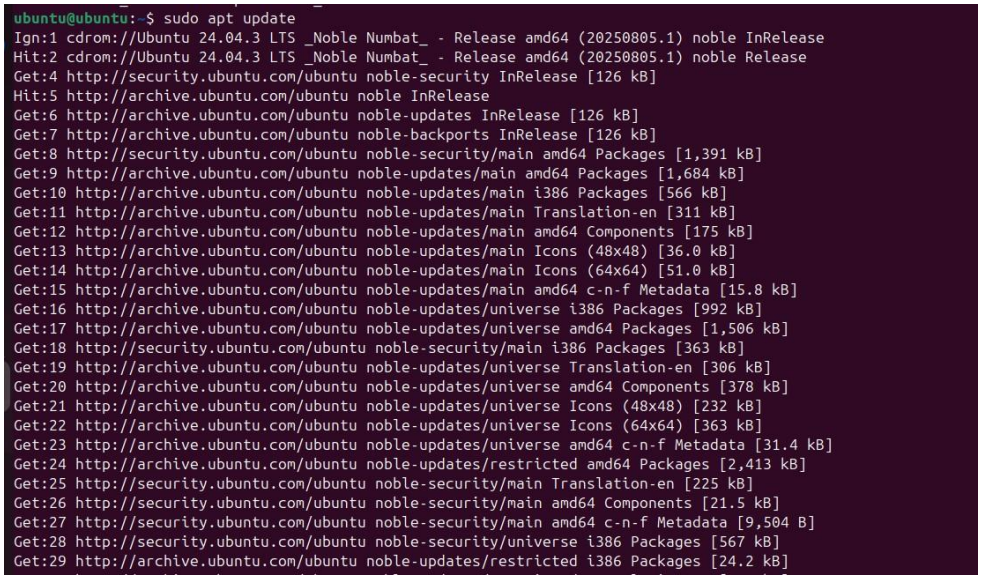


Gambar 2.1 Output Perintah ip a pada Mesin Target (Ubuntu Server)

Gambar 1.2 menunjukkan hasil perintah ip a pada Ubuntu Server, di mana interface ens33 berada dalam keadaan UP dengan alamat IP 192.168.204.129/24 dan broadcast 192.168.204.255, sehingga server target dipastikan berada pada subnet yang sama dengan mesin attacker dan siap digunakan sebagai host layanan DVWA dalam scenario serangan DoS.

F. PERSIAPAN SERVER TARGET

1. Pembaruan Paket Sistem pada Ubuntu Server

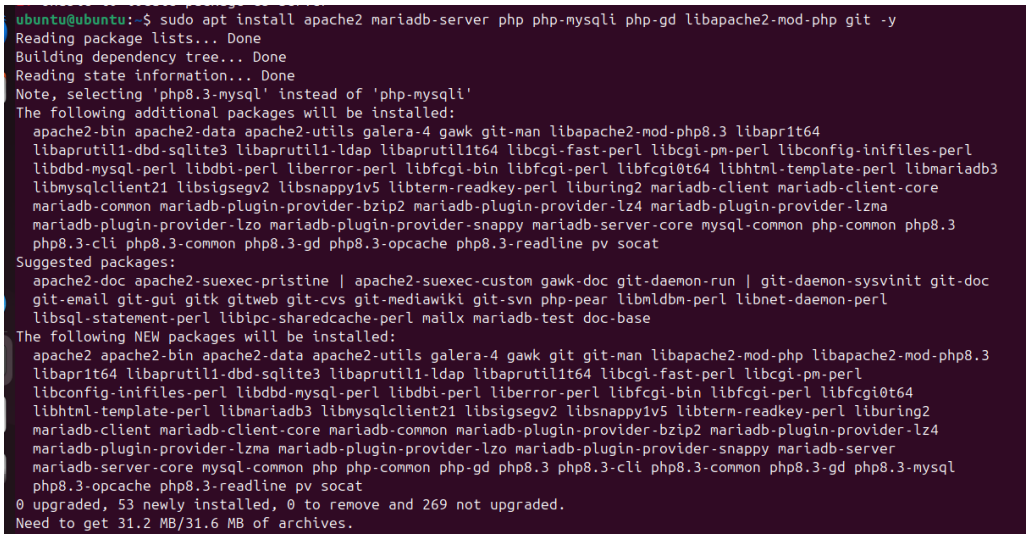


1.3 proses Eksekusi Perintah sudo apt update pada Ubuntu Server

Gambar 1.3 memperlihatkan proses eksekusi perintah sudo apt update pada Ubuntu Server yang sedang mengambil daftar paket terbaru dari repositori resmi Ubuntu agar indeks paket lokal sistem tetap terbarui sebelum instalasi Apache, MariaDB, PHP, dan DVWA dilakukan

2. Instalasi Web Server dan Dependensi

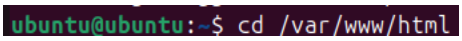
   Ubuntu Server dikonfigurasi sebagai web server menggunakan Apache, MariaDB, PHP, dan Git untuk mendukung aplikasi DVWA.



Gambar 1.4 Proses Instalasi Apache2, MariaDB, PHP, dan Git pada Ubuntu Server

Gambar 1.4 menampilkan eksekusi perintah sudo apt install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php git -y yang menginstal komponen utama LAMP, yaitu Apache2 sebagai web server, MariaDB sebagai database, PHP beserta modul php-mysqli, php-gd, dan libapache2-mod-php untuk menjalankan aplikasi DVWA, serta Git untuk mengunduh source code DVWA dari repositori.

3. Persiapan Direktori Web Root untuk DVWA



Gambar 1.5 Perpindahan Direktori ke /var/www/html sebagai Web Root Apache

Gambar 1.5 memperlihatkan perintah cd /var/www/html yang digunakan untuk berpindah ke direktori web root Apache, yaitu lokasi utama penyimpanan file aplikasi web sehingga nantinya source code DVWA dapat di-clone atau diletakkan langsung di dalam direktori ini agar dapat diakses melalui browser.

4. Instalasi dan Konfigurasi DVWA

   Aplikasi DVWA diunduh dari GitHub dan ditempatkan pada direktori /var/www/html. File konfigurasi database disesuaikan agar DVWA dapat terhubung ke MariaDB.

```
ubuntu@ubuntu:/var/www/html$ sudo git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 5622, done.
remote: Total 5622 (delta 0), reused 0 (delta 0), pack-reused 5622 (from 1)
Receiving objects: 100% (5622/5622), 2.64 MiB | 1.42 MiB/s, done.
Resolving deltas: 100% (2809/2809), done.
```

Gambar 1.6 Proses git clone Repositori DVWA ke Direktori /var/www/html

Gambar 1.6 memperlihatkan perintah sudo git clone https://github.com/digininja/DVWA.git yang digunakan untuk mengunduh seluruh source code DVWA ke dalam direktori web root /var/www/html/DVWA, sehingga aplikasi DVWA siap untuk dikonfigurasi lebih lanjut sebelum digunakan sebagai target serangan DoS

5. Pengaturan Hak Akses Direktori DVWA

```
ubuntu@ubuntu:/var/www/html$ sudo chmod -R 777 /var/www/html/DVWA/
```

Gambar 1.7 Pemberian Izin Akses chmod -R 777 pada Direktori /var/www/html/DVWA

Gambar 1.7 menampilkan perintah sudo chmod -R 777 /var/www/html/DVWA/ yang digunakan untuk memberikan izin baca, tulis, dan eksekusi penuh secara rekursif pada seluruh file dan folder DVWA, sehingga web server Apache dan proses lain dapat mengakses serta memodifikasi berkas DVWA tanpa kendala selama praktikum, meskipun secara keamanan pengaturan 777 ini sangat longgar dan sebaiknya hanya digunakan pada lingkungan lab tertutup.

6. Verifikasi Struktur Direktori Web DVWA

```
ubuntu@ubuntu:/var/www/html$ ls /var/www/html/
DVWA  index.html
```

Gambar 1.8 Hasil Perintah ls /var/www/html/ Menunjukkan Direktori DVWA

Gambar 1.8 memperlihatkan hasil perintah ls /var/www/html/ yang menampilkan direktori DVWA dan berkas index.html, yang menandakan bahwa source code DVWA telah berhasil ditempatkan pada web root Apache dan siap diakses melalui browser menggunakan URL yang mengarah ke direktori DVWA.

7. Konfigurasi File config.inc.php DVWA

```
ubuntu@ubuntu:/var/www/html$ cd DVWA/config
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo cp config.inc.php.dist config.inc.php
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo nano config.inc.php
```

Gambar 1.9 Penyalinan dan Pengeditan File config.inc.php pada Direktori DVWA/config

Gambar 1.9 memperlihatkan langkah masuk ke direktori DVWA/config, kemudian menyalin berkas template config.inc.php.dist menjadi config.inc.php dengan perintah sudo cp config.inc.php.dist config.inc.php, dan selanjutnya membuka file tersebut menggunakan sudo nano config.inc.php untuk menyesuaikan parameter koneksi database serta pengaturan lain yang dibutuhkan DVWA sebelum proses setup database dijalankan

8. Pembuatan Database dan User DVWA pada MariaDB

Database DVWA dibuat dan diinisialisasi melalui halaman *Database Setup*, hingga halaman login DVWA dapat diakses secara normal melalui browser.

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo mariadb
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.13-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> CREATE USER 'andinifebrianti'@'localhost' IDENTIFIED BY '11111';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> CREATE ALL PRIVILEGES ON dvwa.* TO 'andinifebrianti'@'localhost';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server versi
on for the right syntax to use near 'ALL PRIVILEGES ON dvwa.* TO 'andinifebrianti'@'localhost'' at line 1
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'andinifebrianti'@'localhost';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> EXIT
Bye
```

Gambar 1.10 Perintah CREATE DATABASE, CREATE USER, GRANT ALL PRIVILEGES, dan FLUSH PRIVILEGES untuk DVWA di MariaDB

Gambar 1.10 menampilkan sesi MariaDB yang digunakan untuk membuat database dvwa, membuat user database baru dengan perintah CREATE USER 'andnifebrianti'@'localhost' IDENTIFIED BY '11111';, kemudian memberikan hak akses penuh ke database DVWA melalui GRANT ALL PRIVILEGES ON dvwa.* TO 'andnifebrianti'@'localhost';, diikuti FLUSH PRIVILEGES; agar perubahan hak akses langsung berlaku dan DVWA dapat terhubung ke database menggunakan kredensial tersebut.

G. KONDISI KERENTANAN SISTEM

Agar dampak serangan dapat diamati dengan jelas, dilakukan pelemahan sistem secara sengaja, antara lain:

1. Menonaktifkan UFW Firewall.

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo ufw disable
Firewall stopped and disabled on system startup
```

Gambar 1.11 Menonaktifkan UFW Firewall pada Server Target

Gambar 1.11 memperlihatkan eksekusi perintah sudo ufw disable yang menghasilkan pesan "Firewall stopped and disabled on system startup", yang berarti firewall UFW dinonaktifkan sepenuhnya sehingga tidak lagi memfilter trafik jaringan, sehingga kondisi sistem menjadi lebih rentan dan sesuai dengan kebutuhan praktikum untuk mengamati dampak serangan DoS tanpa perlindungan firewall bawaan Ubuntu.

2. Menonaktifkan TCP SYN Cookies.

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

Gambar 1.12 Perintah sudo sysctl -w net.ipv4.tcp_syncookies=0 untuk Mematikan Proteksi SYN Cookies

Gambar 1.12 menunjukkan perintah sudo sysctl -w net.ipv4.tcp_syncookies=0 yang mengubah parameter kernel net.ipv4.tcp_syncookies menjadi 0, sehingga mekanisme SYN cookies sebagai perlindungan bawaan terhadap serangan SYN Flood dinonaktifkan dan membuat server lebih rentan terhadap penumpukan koneksi setengah-terbuka selama percobaan serangan DoS.

3. Menurunkan nilai tcp_max_syn_backlog.

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo sysctl -w net.ipv4.tcp_max_syn_backlog=10
net.ipv4.tcp_max_syn_backlog = 10
```

Gambar 1.13 Menurunkan Nilai tcp_max_syn_backlog untuk Memperlemah Antrian SYN

Gambar 1.13 menampilkan perintah sudo sysctl -w net.ipv4.tcp_max_syn_backlog=10 yang menurunkan batas maksimum antrian koneksi TCP dalam status SYN_RECV menjadi 10, sehingga server hanya dapat mengingat sedikit koneksi setengah-terbuka sebelum mulai menjatuhkan paket baru, membuat

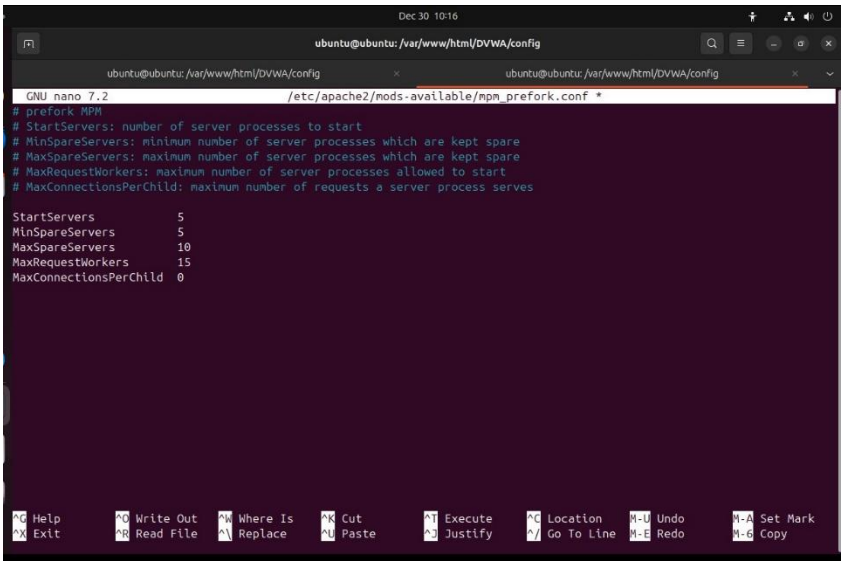
layanan web jauh lebih rentan terhadap serangan SYN Flood dan memudahkan observasi dampak DoS dalam praktikum.

4. Membatasi MaxRequestWorkers pada Apache.

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo nano /etc/apache2/mods-available/mpm_prefork.conf
```

Gambar 1.15 Pengaturan Batas Proses Apache melalui mpm_prefork.conf

Gambar 1.5 menunjukkan perintah sudo nano /etc/apache2/mods-available/mpm_prefork.conf yang digunakan untuk membuka konfigurasi modul Apache MPM Prefork, di mana parameter seperti StartServers, MinSpareServers, MaxSpareServers, dan terutama MaxRequestWorkers dapat disesuaikan untuk membatasi jumlah proses Apache yang melayani permintaan, sehingga dalam konteks praktikum ini nilainya dapat diturunkan agar layanan menjadi lebih sensitif terhadap serangan Slowloris dan DoS berbasis koneksi.

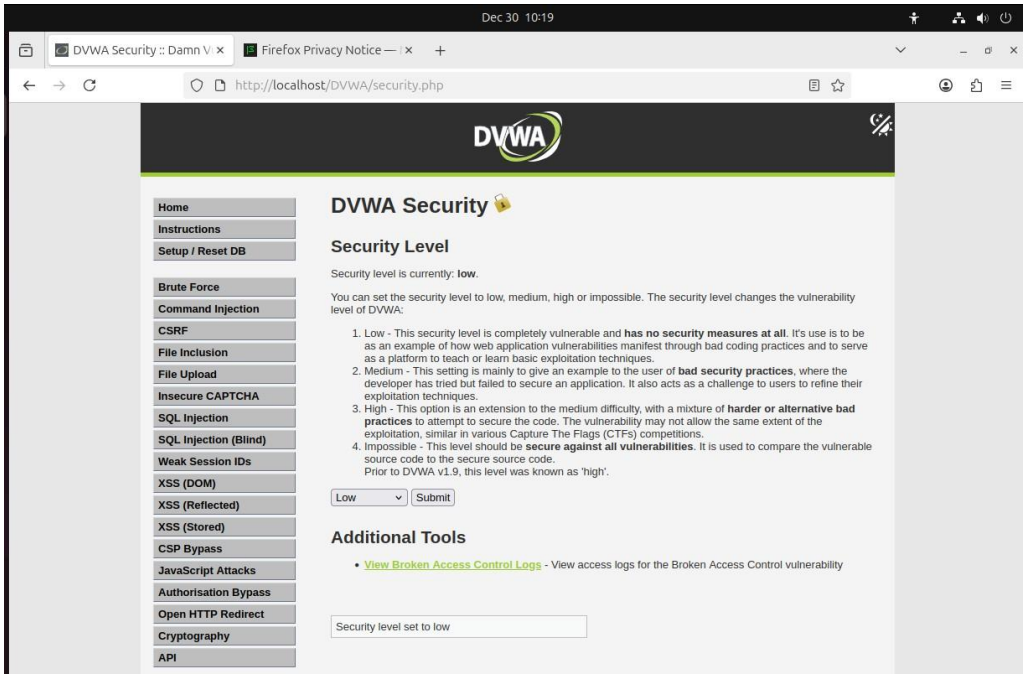


Gambar 1.16 Pengaturan Batas Proses Apache melalui mpm_prefork.conf

Gambar 1.16 menunjukkan perintah sudo nano /etc/apache2/mods-available/mpm_prefork.conf yang digunakan untuk membuka konfigurasi modul Apache MPM Prefork, di mana parameter seperti StartServers, MinSpareServers, MaxSpareServers, dan

terutama MaxRequestWorkers dapat disesuaikan untuk membatasi jumlah proses Apache yang melayani permintaan, sehingga dalam konteks praktikum ini nilainya dapat diturunkan agar layanan menjadi lebih sensitif terhadap serangan Slowloris dan DoS berbasis koneksi.

5. Mengatur DVWA Security Level ke level rendah.



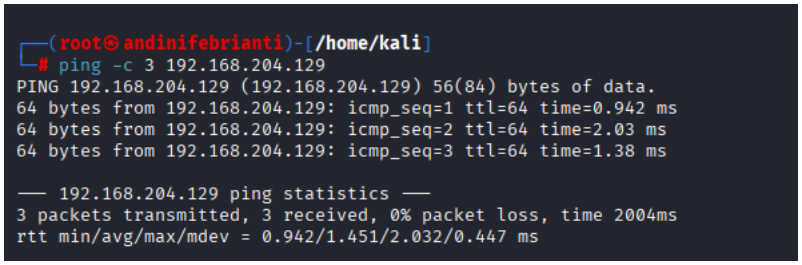
Gambar 1.17 Tampilan Halaman "DVWA Security" dengan Security Level Diset ke low

Gambar 1.17 menunjukkan halaman "DVWA Security" pada browser Firefox, di mana opsi Security Level ditampilkan sebagai low dan dapat diubah melalui tombol Submit, yang berarti seluruh modul kerentanan DVWA dikonfigurasi pada tingkat keamanan terendah sehingga berbagai serangan web, termasuk DoS pada layer aplikasi, dapat dieksploitasi dengan lebih mudah selama praktikum.

H. PENGUJIAN KONDISI NORMAL (BASELINE)

Sebelum serangan dilakukan:

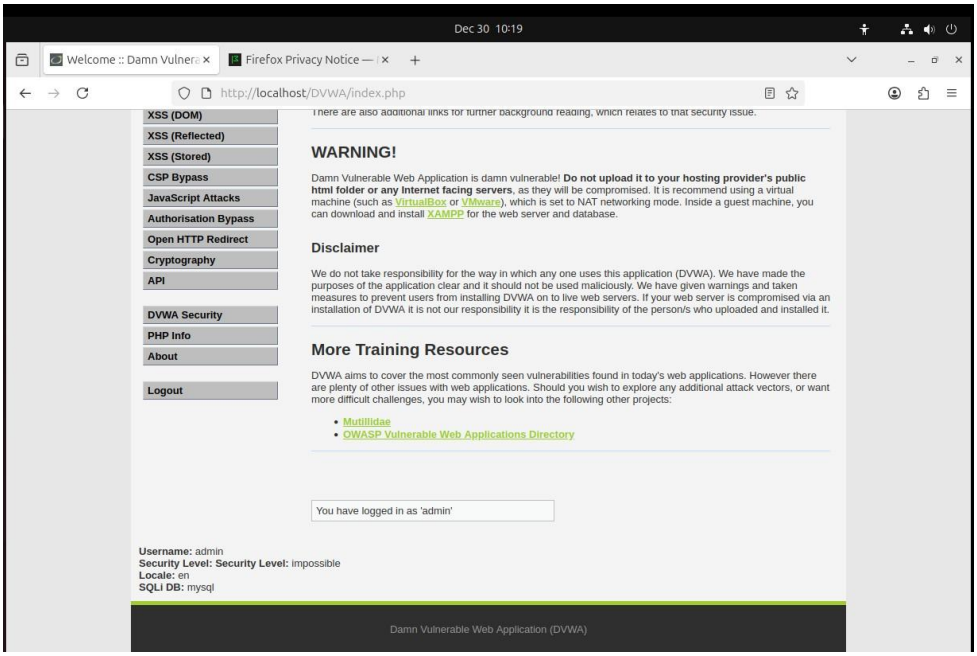
- Ping dari attacker ke target berhasil tanpa packet loss.



Gambar 1.18 Hasil Perintah ping -c 3 192.168.204.129 dari Mesin Kali ke Server Ubuntu

Gambar 1.18 memperlihatkan output perintah ping -c 3 192.168.204.129 dari mesin attacker (Kali) yang menunjukkan tiga balasan ICMP dari server target dengan waktu respon sekitar 0,94–2,03 ms dan statistik akhir "3 packets transmitted, 3 received, 0% packet loss", yang menandakan konektivitas jaringan antara attacker dan server DVWA dalam kondisi normal dan stabil sebelum serangan DoS dijalankan.

- Akses web DVWA berjalan normal dan halaman login dapat dimuat dengan cepat.

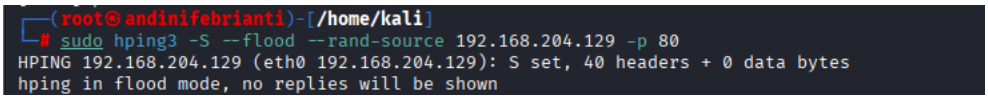


Gambar 1.19 Tampilan Halaman Utama DVWA (index.php) Setelah Login sebagai admin

Gambar 1.19 memperlihatkan halaman utama DVWA pada browser Firefox dengan status “You have logged in as 'admin'” di bagian bawah serta informasi Security Level: impossible, yang menunjukkan bahwa aplikasi DVWA dapat diakses dan digunakan secara normal sebelum dilakukan perubahan tingkat keamanan dan serangan DoS, sehingga kondisi ini dijadikan baseline untuk membandingkan dampak serangan terhadap ketersediaan layanan

I. SIMULASI SERANGAN DOs

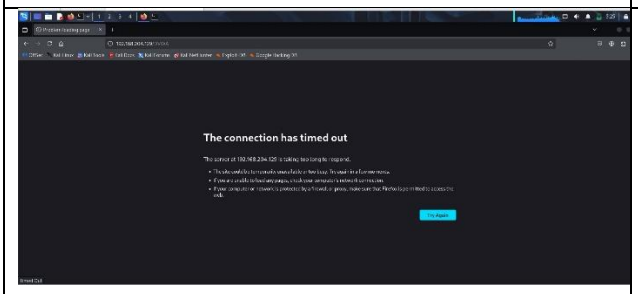
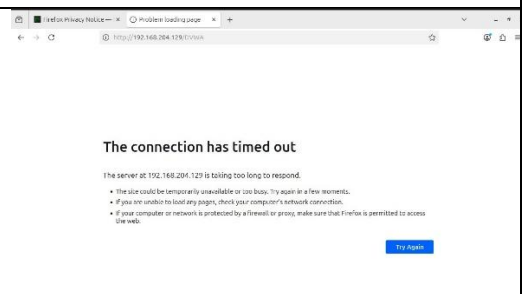
1. Serangan SYN Flood (Hping3)



Gambar 1.20 Perintah sudo hping3 -S --flood --rand-source 192.168.204.129 -p 80 untuk Melakukan Serangan SYN Flood

Gambar 1.20 menunjukkan eksekusi perintah sudo hping3 -S --flood --rand-source 192.168.204.129 -p 80 dari mesin Kali, yang mengirim paket TCP dengan flag SYN ke port 80 server secara terus-menerus dan secepat mungkin dengan sumber IP acak, sehingga antrian koneksi setengah-terbuka pada server web penuh dan mengakibatkan gangguan ketersediaan layanan DVWA bagi pengguna sah.

2. Dampak Serangan SYN Flood terhadap Akses DVWA

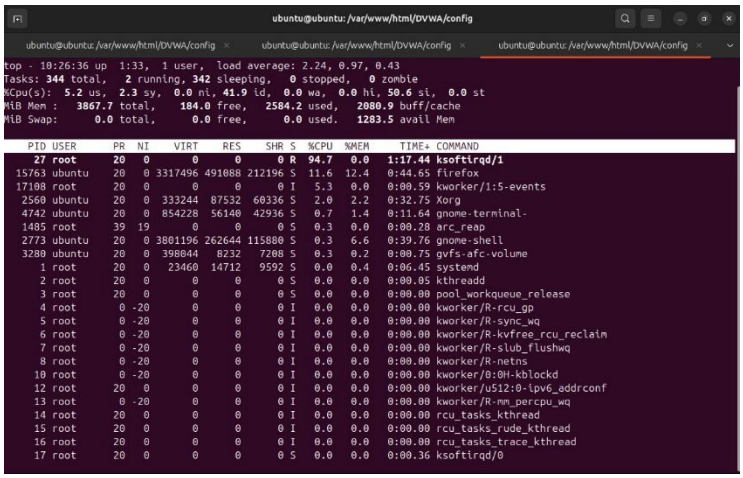
Firefox kali linux	Firefox ubuntu
	

Gambar 1.21 Halaman Firefox pada Kali Linux dan Ubuntu Menampilkan Pesan “The connection has timed out”

Gambar 1.21 memperlihatkan dua jendela Firefox, masing-masing di mesin Kali Linux (attacker) dan Ubuntu (client lain), yang keduanya gagal memuat halaman DVWA

dan menampilkan pesan “The connection has timed out”, yang menunjukkan bahwa serangan SYN Flood ke port 80 telah menghabiskan kapasitas koneksi Apache sehingga baik penyerang maupun pengguna sah tidak dapat lagi mengakses layanan web selama antrian koneksi server tersaturasi.

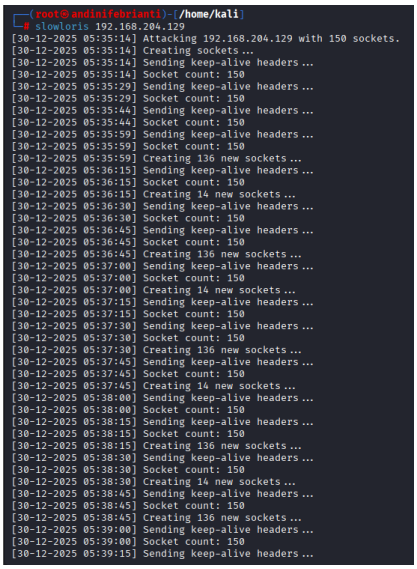
3. Pemantauan Beban CPU Server saat Serangan SYN Flood



Gambar 1.22 Output Perintah top pada Ubuntu Server Menunjukkan Kenaikan Load Average dan Proses ksoftirqd

Gambar 1.22 memperlihatkan hasil perintah top di server Ubuntu ketika serangan SYN Flood berlangsung, dengan nilai load average yang meningkat dan proses kernel seperti ksoftirqd serta proses terkait jaringan lain mengonsumsi persentase CPU yang tinggi, yang menunjukkan bahwa penanganan interrupt jaringan akibat banjir paket SYN membebani resource CPU dan mengurangi kemampuan server untuk memproses permintaan web yang sah.

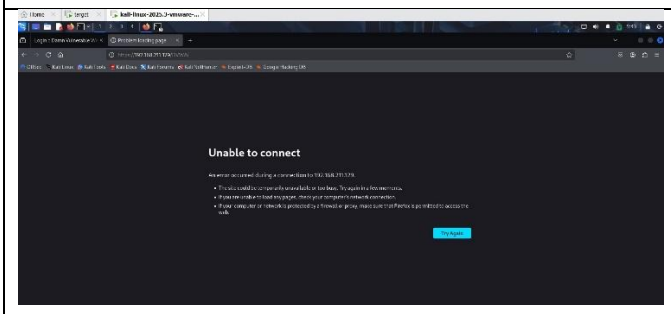
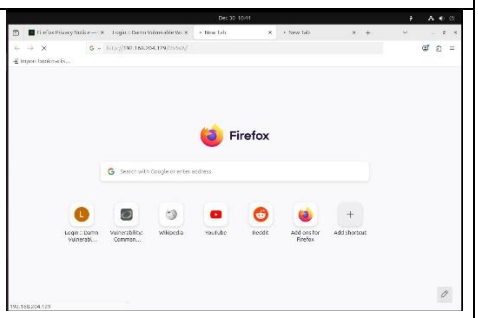
4. Serangan Slowloris



Gambar 1.23 Eksekusi Serangan Slowloris pada Layer Aplikasi

Gambar 1.23 memperlihatkan jalannya skrip Slowloris yang terus-menerus membuat socket HTTP baru ke alamat 192.168.204.129 dan mengirim header keep-alive secara berkala, sehingga jumlah socket aktif dipertahankan di sekitar 150 koneksi terbuka dan tidak pernah ditutup, yang menyebabkan seluruh slot koneksi Apache habis dan layanan DVWA tetap hidup namun tidak lagi dapat merespons permintaan HTTP baru dari klien sah

5. Dampak Serangan Slowloris terhadap Akses Pengguna

Firefox kali linux	Firefox ubuntu
	

Gambar 1.24 Perbandingan Tampilan Firefox di Kali Linux dan Ubuntu Saat Serangan Slowloris

Gambar 1.24 memperlihatkan bahwa pada sisi attacker (Firefox di Kali Linux) muncul pesan “Unable to connect” ketika mencoba mengakses DVWA, sementara browser Firefox di mesin Ubuntu hanya menampilkan halaman awal tanpa berhasil memuat situs

DVWA, yang menunjukkan bahwa seluruh koneksi Apache telah terkunci oleh serangan Slowloris sehingga baik penyerang maupun klien sah tidak lagi dapat membuka halaman aplikasi web.

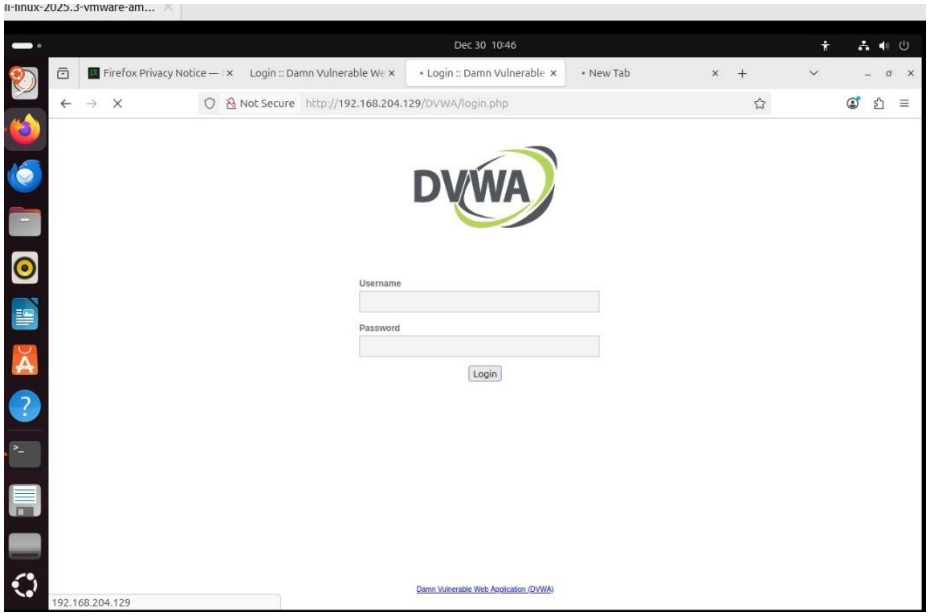
J. PENERAPAN MITIGASI FIREWALL

1. Mitigasi SYN Flood

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

Gambar 1.25 Aturan iptables dengan Modul limit untuk Membatasi Paket TCP SYN

Gambar 1.25 menampilkan perintah sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT yang menambahkan aturan pada chain INPUT untuk hanya menerima rata-rata satu paket TCP dengan flag SYN per detik, sehingga koneksi baru ke server dibatasi kecepatannya dan serangan seperti SYN Flood maupun pembukaan koneksi berlebihan menjadi lebih sulit menghabiskan kapasitas antrian koneksi kernel



Gambar 1.26 Tampilan Halaman Login DVWA pada Firefox Setelah Aturan Firewall untuk hping3 Diterapkan

Gambar 1.26 memperlihatkan bahwa setelah penerapan aturan IPTables yang membatasi laju koneksi HTTP, halaman login DVWA kembali dapat dimuat secara normal di browser Firefox pada Ubuntu dengan URL http://192.168.204.129/DVWA/login.php, yang menandakan bahwa mekanisme rate

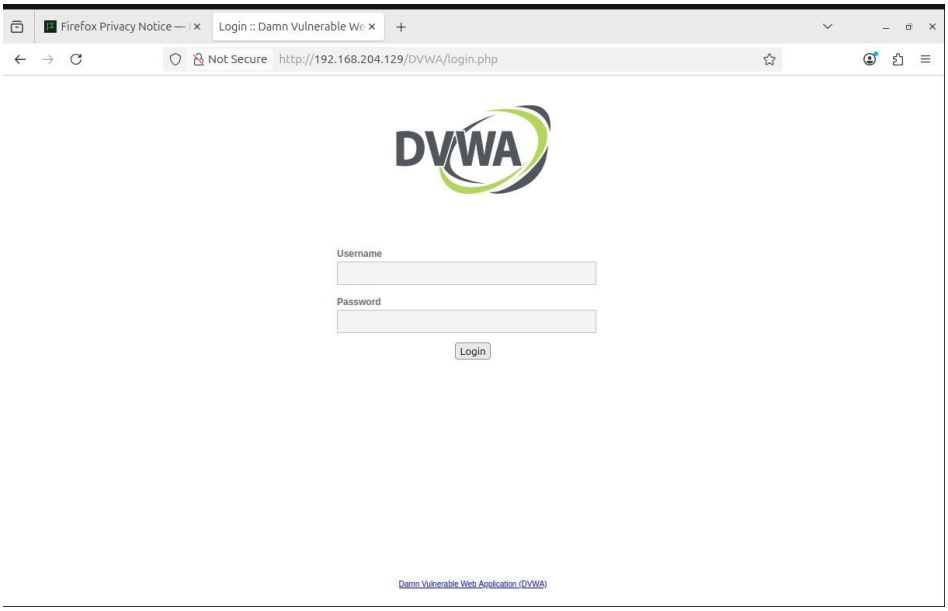
limiting berhasil mengurangi koneksi gantung dari Slowloris sehingga slot koneksi Apache kembali tersedia bagi pengguna sah

2. Mitigasi SlowlorisDiterapkan pembatasan laju koneksi TCP menggunakan modul limit. Teknik ini berhasil mengurangi koneksi berlebih dan memulihkan ketersediaan layanan web.

```
ubuntu@ubuntu:/var/www/html/DVWA/config$ sudo iptables -A INPUT -s 192.168.204.128 -j DROP
```

Gambar 1.27 Aturan iptables untuk Men-drop Seluruh Trafik dari IP 192.168.204.128

Gambar 1.27 menampilkan perintah sudo iptables -A INPUT -s 192.168.204.128 -j DROP yang menambahkan aturan pada chain INPUT untuk menjatuhkan semua paket yang berasal dari alamat IP attacker 192.168.204.128, sehingga setiap percobaan koneksi baru (termasuk serangan SYN Flood maupun Slowloris) dari mesin tersebut langsung diblokir di sisi firewall dan tidak lagi mencapai layanan web DVWA.



Gambar 1.28 Tampilan Halaman Login DVWA yang Kembali Normal pada Browser Firefox

Gambar 1.28 memperlihatkan bahwa setelah aturan IPTables diterapkan untuk memblokir IP attacker, halaman login DVWA pada alamat http://192.168.204.129/DVWA/login.php kembali dapat diakses oleh klien Ubuntu tanpa gangguan, yang menunjukkan bahwa pemblokiran sumber serangan di firewall

berhasil memulihkan ketersediaan layanan web bagi pengguna sah sementara trafik berbahaya tetap terfilter.

K. HASIL DAN ANALISIS

- Serangan SYN Flood berdampak langsung pada layer jaringan dengan meningkatkan beban CPU dan antrean koneksi.
- Serangan Slowloris efektif melumpuhkan layanan pada layer aplikasi tanpa mematikan server.
- IPTables terbukti efektif sebagai mekanisme mitigasi dasar untuk membedakan trafik sah dan berbahaya.

L. KESIMPULAN

Berdasarkan hasil praktikum dapat disimpulkan bahwa:

1. Serangan DoS baik pada network layer maupun application layer mampu melumpuhkan layanan web DVWA.
2. Konfigurasi keamanan kernel dan Apache sangat berpengaruh terhadap keberhasilan serangan.
3. Firewall IPTables dapat digunakan sebagai solusi mitigasi awal untuk menjaga ketersediaan layanan.
4. Simulasi ini memberikan gambaran nyata mengenai pentingnya perlindungan terhadap serangan DoS dalam sistem jaringan.